UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/814,983 | 03/31/2004 | Hashem Mohammad Ebrahimi | 1565.069US1 | 9751 |

21186          7590          07/09/2008
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

| EXAMINER |
|---|
| GYORFI, THOMAS A |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/09/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _30 April 2008_.
2a)☐ This action is **FINAL**.            2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _1,2,4-15,17-22 and 24-26_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1,2,4-15,17-22 and 24-26_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____ .

## DETAILED ACTION

1.      Claims 1, 2, 4-15, 17-22, and 24-26 remain for examination.  The

correspondence filed 4/30/08 amended claims 1, 8, 15, 21, & 24; and cancelled claims

3, 16, and 23.

### *Continued Examination Under 37 CFR 1.114*

2.      A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection.  Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114.  Applicant's submission filed on 4/30/08

has been entered.

### *Response to Arguments*

3.      With respect to the Netscape reference, Applicant argues on pages 7-8 of the

amendment:

> Here, the Netscape reference (specifically the primary chapter (14) recited by the
> Examiner) details a technique to set up a reverse proxy via a Netscape browser to
> authenticate client communications and content server communications. However, the
> client authenticates to the Netscape proxy and then the Netscape proxy authenticates to
> the content server. In other words, the Netscape proxy does not authenticate the content
> server, it is the other way around in the cited reference, such that it is the content server
> that authenticates the proxy. The Applicant invites the Examiner to re-review chapter 14
> of the Netscape reference to validate this contention of the Applicant where it is clearly
> seen the content server is the one that authenticates the proxy and not the other way
> around.

Examiner fails to see how this argument has any relevance to the claimed

subject matter, as these details are not found anywhere in the claims.  The only

requirement recited in the claims with respect to communication between the local

domain accelerator and the content server is that they establish a separate "secure"

communication between each other; but there is absolutely no mention of who

authenticates whom.  Moreover, the instant specification, while providing a minimum

level of detail as to the nature of the secure communication (page 8, lines 3-10 & 18-27;

page 13, lines 11-26), fails to disclose how or even if either party is required to

authenticate to the other in order to establish said secure communication.  Thus, even

assuming *arguendo* that the specification could be relied on to make such a distinction,

it would be irrelevant as limitations from the specification are not read into the claims.

See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant's remaining arguments with respect to claims 1-26 have been

considered but are moot in view of the new ground(s) of rejection.  For the sake of

brevity and to expedite prosecution of the case, Examiner has voluntarily withdrawn the

redundant rejections under 35 USC 103(a) using the Birrell reference.  This is not to be

construed as an admission that the instant application is allowable over Birrell (in view

of the references listed herein); and Examiner reserves the right to reinstate rejections

using the Birrell reference as may be warranted by future amendments to the claims.

## *Claim Rejections - 35 USC § 103*

4.      The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

5.      Claims 1, 2, 4-15, 17-22, and 24-26 are rejected under 35 U.S.C. 103(a) as being

unpatentable over "The Netscape Proxy Server Version 3.5 for Unix Administrator's

Guide" (hereinafter, "Netscape") in view of Davis (U.S. Patent Application Publication

2002/0199098).


Regarding claim 1:

        Netscape discloses a method comprising: receiving a secure communication

request from a client (Chapter 14, page 2, Figure 14.1 and 1st paragraph); identifying a

domain identification associated with the request (inherent to proxying in general; cf.

Chapter 6, e.g. "Enabling Proxying for a Resource"); and routing the request to a proxy

based on the domain identification, wherein the proxy communicates securely with the

external domain via a first set of unique session keys used for the local domain

accelerator and the external domain (Chapter 14, "Setting up Client Authentication in a

Reverse Proxy", cf. "Content Server Authenticates Proxy") and separately the local

domain accelerator communicates securely with the client via a second set of unique

session keys used for the local domain accelerator and the client to communicate

(Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Proxy

Authenticates Client") and the first set of session keys and the second set of session

keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL

connections disclosed) and wherein the client believes communication that the client

has with the local domain accelerator is occurring with the external domain but in fact it

occurs with the local domain accelerator via the second set of session keys ("What

Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 7, "How Reverse

Proxying Works"), and wherein the local domain accelerator caches data from the

external domain for servicing the request of the client (see all of Chapter 9, beginning

with "How Caching Works").

Netscape appears to be silent regarding wherein the local domain accelerator

vends an external domain certificate to the client during the communication to present

itself as the external domain.  However, Davis discloses an analogous SSL enabled

proxy server wherein the proxy stores the server's authentication certificate and vends it

to the client during the SSL negotiation phase between the client and the proxy

(paragraph 0016).  It would have been obvious to modify the Netscape proxy server to

use the external domain's certificate in negotiating the SSL connection between itself

and the client, because the technique was clearly a known improvement that was well

within the capabilities of one of ordinary skill in the art, in view of the teaching of the

technique in an equivalent proxy server.


Regarding claim 8:

Netscape discloses a method comprising: receiving a secure request forwarded

from a proxy, the secure request originating from a client and destined for an external

domain (Chapter 14, page 2, Figure 14.1 and 1st paragraph); establishing a secure

communication with the client by providing the client a certificate associated with an

external domain (Chapter 5, "Controlling Access with Client Certificates") and wherein

the secure communication entails using a first set of session keys to communicate

securely with the client and the client believes after receiving the certificate that

communication is occurring with the external domain (Chapter 14, "Setting up Client

Authentication in a Reverse Proxy", cf. "Proxy Authenticates Client"; Chapter 7, "How

Reverse Proxying Works"); and servicing the client with data that is acquired from the

external domain, and wherein a portion of that data is used to service the request (all of

Chapter 9), and wherein separate communication is securely established with the

external domain using a second set of session keys different from the first set of session

keys (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Content

Server Authenticates Proxy").

Netscape appears to be silent regarding wherein the certificate is for the external

domain and is vended to the client to make the client believe the secure interaction is

occurring with the external domain.  However, Davis discloses an analogous SSL

enabled proxy server wherein the proxy stores the server's authentication certificate and

vends it to the client during the SSL negotiation phase between the client and the proxy

(paragraph 0016).  It would have been obvious to modify the Netscape proxy server to

use the external domain's certificate in negotiating the SSL connection between itself

and the client, because the technique was clearly a known improvement that was well

within the capabilities of one of ordinary skill in the art, in view of the teaching of the

technique in an equivalent proxy server.


Regarding claim 15:

Netscape discloses a system comprising: a proxy (e.g. "What Netscape Proxy Server Provides"); and a local domain accelerator (Ibid, but particularly the 3$^{rd}$ and 4$^{th}$ paragraphs; cf. Chapter 9, "How Caching Works") wherein a client securely requests an external domain and the proxy routes the request to the local domain accelerator [i.e. itself], the local domain accelerator securely communicates with the external domain and services the client via secure communications between the local domain accelerator and the client (Chapter 14, e.g. "Tunneling SSL through the Proxy Server"), and wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Content Server Authenticates Proxy") and separately the local domain accelerator communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client to communicate (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Proxy Authenticates Client") and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides", 2$^{nd}$ and 5$^{th}$ paragraphs; Chapter 7, "How Reverse Proxying Works").

Netscape appears to be silent regarding wherein the local domain accelerator vends an external domain certificate to the client during the communication to present

itself as the external domain. However, Davis discloses an analogous SSL enabled

proxy server wherein the proxy stores the server's authentication certificate and vends it

to the client during the SSL negotiation phase between the client and the proxy

(paragraph 0016). It would have been obvious to modify the Netscape proxy server to

use the external domain's certificate in negotiating the SSL connection between itself

and the client, because the technique was clearly a known improvement that was well

within the capabilities of one of ordinary skill in the art, in view of the teaching of the

technique in an equivalent proxy server.


Regarding claim 21:

Netscape discloses a system comprising: a local domain accelerator ("What

Netscape Proxy Server Provides", 3rd and 4th paragraphs; Chapter 9, "How Caching

Works"); and wherein the local domain accelerator securely communicates with a client

as if the local domain accelerator was an external domain [i.e. a proxy] and securely

communicates with the external domain for purposes of acquiring data from the external

domain (Chapter 14, e.g. "Tunneling SSL through the Proxy Server"), wherein the proxy

communicates securely with the external domain via a first set of unique session keys

used for the local domain accelerator and the external domain (Chapter 14, "Setting up

Client Authentication in a Reverse Proxy", cf. "Content Server Authenticates Proxy") and

separately the local domain accelerator communicates securely with the client via a

second set of unique session keys used for the local domain accelerator and the client

to communicate (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf.

"Proxy Authenticates Client") and the first set of session keys and the second set of

session keys are different from one another (Ibid, by virtue of being inherent to the

multiple SSL connections disclosed) and wherein the client believes communication that

the client has with the local domain accelerator is occurring with the external domain but

in fact it occurs with the local domain accelerator via the second set of session keys

("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 7, "How

Reverse Proxying Works").

     Netscape appears to be silent regarding wherein the local domain accelerator

vends an external domain certificate to the client during the communication to present

itself as the external domain. However, Davis discloses an analogous SSL enabled

proxy server wherein the proxy stores the server's authentication certificate and vends it

to the client during the SSL negotiation phase between the client and the proxy

(paragraph 0016). It would have been obvious to modify the Netscape proxy server to

use the external domain's certificate in negotiating the SSL connection between itself

and the client, because the technique was clearly a known improvement that was well

within the capabilities of one of ordinary skill in the art, in view of the teaching of the

technique in an equivalent proxy server.


Regarding claims 2 and 19:

     Netscape further discloses one of a forward proxy and a transparent proxy

("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 14, "Using

Encryption in the Proxy Server, 2nd paragraph).

Regarding claims 4 and 18:

Netscape further discloses establishing a Secure Sockets Layer (SSL)

handshake between the client and the local domain accelerator to service the request,

wherein the client believes that the handshake is with external domain (Chapter 14).

Regarding claim 5:

Netscape further discloses intercepting the request that originates from the client

to the external domain (inherent to proxies by definition; see also Chapter 6, "Sending

the Client's IP Address to the Server", wherein by default the proxy intercepts a client

request to replace the client's IP address with the proxy's IP address).

Regarding claims 6 and 10:

Netscape further discloses accessing, by the local domain accelerator, caching

services for caching and managing the data (all of Chapter 9).

Regarding claim 7:

Netscape further discloses wherein stripping a host header from the request,

host header being the domain identifier that identifies the external domain (inherent to

proxies by definition; see also Chapter 5, "Allowing Access to a Resource").

Regarding claim 9:

Netscape further discloses acting as the external domain when interacting with the client (inherent to being a transparent proxy: "What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 14, "Using Encryption in the Proxy Server, 2nd paragraph).

Regarding claim 11:

Netscape further discloses acquiring at least a portion of the data from the external domain in advance of a subsequent request for that portion of the data, wherein the subsequent request is issued from the client (Chapter 9, "Using Cache Batch Updates").

Regarding claim 12:

Netscape further discloses interacting securely with the external domain to acquire the data housed in the local cache (Ibid; secure connections disclosed in Chapter 14, e.g. "Setting Up Client Authentication in a Reverse Proxy").

Regarding claims 13 and 17:

Netscape further discloses wherein interacting securely further includes mutually signing interactions transmitted between the local domain accelerator and the external domain, as this is inherent to SSL ("The Secure Socket Layer Protocol (SSL)", page 3, "SSL – Authentication and Integrity"; cf. Netscape, Chapter 5, "Controlling Access with Client Certificates"; see also RFC2246, e.g. page 41).

Regarding claim 14:

Netscape further discloses using the proxy to establish a secure communications

channel between the local domain accelerator and the external domain (Chapter 14,

e.g. Figure 14.2 and "Setting Encryption Preferences").

Regarding claims 20 and 22:

Netscape further discloses wherein the proxy creates a secure communications

tunnel between the client and the local domain accelerator and the proxy creates a

secure communications channel between the local domain accelerator and the external

domain (Chapter 7, "Setting Up a Secure Reverse Proxy"; Chapter 14, "Setting up

Client Authentication in a Reverse Proxy").

Regarding claim 24:

SSL as implemented by Netscape inherently requires an exchange of certificates

during communications between two parties (see "The Secure Sockets Layer Protocol

(SSL)", page 3, "SSL – Authentication and Integrity"; cf. Netscape, Chapter 5,

"Controlling Access with Client Certificates"; see also RFC2246, page 23).

Regarding claim 25:

Netscape further discloses wherein the client is a browser using SSL (e.g.

Netscape Navigator: "What Netscape Proxy Server Provides", 6th paragraph; Chapter

14, "What is HTTPS?"), and the local domain accelerator intercepts and forwards

communications toward a proxy and the proxy forwards communications to the local

domain accelerator where the local domain accelerator presents itself securely to the

client as if it were the external domain (Chapter 6, "Mapping URLs to Other URLs";

Chapter 7, "How Reverse Proxying Works" and "Setting Up a Secure Reverse Proxy").


Regarding claim 26:

Netscape further discloses a plurality of external sites featuring a plurality of

services (e.g. Chapter 7, "Proxying for Load Balancing").


### *Conclusion*

6.      The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure: WO 2002/102020 A1 (the PCT of Davis above).

7.      Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-

3849.  The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859.  The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system.  Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


TAG
7/2/08
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135